REMARKS/ARGUMENTS

To fix antecedent issues, all references to “encoded” key are revised to “encrypted” in the dependent claims. For example, Claim 6 recites “encoded”, but the base Claim 1 actually recites “encrypted” key. Similarly, Claim 16 recites “encoded” which then became “encrypted”; so for uniformity, the only instance of “encoded” key is changed to “encrypted”. No new matter is introduced.

Claim Objections

Claim 2 was objected to because of the following informalities: "wherein digital certificate comprises contains" (line 2) should be changed to "wherein the digital certificate contains".
Claim 2 is amended accordingly.

Claim Rejections - 35 USC § 112

Claim 4 was rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. For examination purpose, the limitation was interpreted as "wherein the digital certificate further contains a signature for selected fields of the digital certificate".
The claim is amended accordingly. Claim 4 is also amended to recite “hashed”, found in paragraph [0035] or Fig. 2, for example.

Claims 7-15 were rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 7 recites the limitation "the

electronic file" in 8. There is insufficient antecedent basis for this limitation in the claim.

Claim 7 is amended to recite “an electronic file”.

Claims 1-15 were rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
The Examiner stated “Claim 1 fails … to recite the interrelationship between the elements as defined in the specification: the key is used to sign the file certificate, the file is encrypted using the key, the file cannot be accessed until the file certificate is verified using the key and the encrypted file is decrypted using the key (figures 10-11 and corresponding text)”.
Claims 1 and 7 are amended accordingly. The encryption of the electronic file is optional (paragraph [00100] 2nd sentence and also the MUX 256 in fig. 10) and therefore the word “optionally” is included. Claim 16 is also amended to include “optionally”.

The Examiner rejected Claim 2 which recites "a software signature" (line 2), stating “there is no software recited in either claim 2 or independent claim 1; and claim 2 fails to recite the interrelationship between the software signature and other elements of the claim as defined by Applicant in the specification: the software signature being a signature for the electronic file that is symmetrically encrypted using the random key (fig. 10). Claim 8 is rejected on the same basis as claim 2.”
Claims 2 and 8 are amended accordingly.

Claim Rejections - 35 USC § 102

Claim 16 was rejected under 35 U.S.C. 102(b) as being anticipated by Ehrsam et al. (4,238,854).

Claim 16 is amended to recite "binding firmware to the computing device by an asymmetric manufacture certificate in the externally-accessible memory". Support is found in paragraph [0045] which describes the public and private key pair (i.e. asymmetric system) and paragraph [0032] which describes the purpose. No new matter is introduced. Such asymmetric manufacture certificate is not taught nor suggested by Ehrsam. Further, Claim 16 recites "optional" encryption, not taught by Ehrsam. Therefore, Claim 16 is believed allowable over Ehrsam. Claim 17 should also be allowable over Ehrsam by virtue of its dependency.

Claim Rejections - 35 USC § 103

Claims 1, 5-7 and 11-13 were rejected under 35 U.S.C. 103(a) as being unpatentable over Ehrsam in view of Pham et al. (6,931,530).

The independent claims, Claim 1, 7 and 16 are amended to include an externally-accessible memory further comprising an asymmetric manufacture certificate to bind firmware to the processing system. Support is found in paragraph [0045] which describes the public and private key pair (i.e. asymmetric system) and paragraph [0032] which describes the purpose. No new matter is introduced. Such an asymmetric manufacture certificate is not taught or suggested by Ehrsam, Pham or Ellison. These independent claims also recite "optional" (MUX, switch) encryption that is not taught in the

references. Yet further, Applicants submit that the combination of references do not provide a working system because they have contrary systems to encrypt the same thing: Ehrsam and Ellison are symmetric whereas Pham is asymmetric.

Therefore, the independent claims 1, 7, 16 (currently amended) are believed allowable over the three references. Dependent claims 2 – 6 on 1, claims 8 – 15 on 7, and 17 on 16 are believed allowable for the at least same reasons.

New Claims

New independent Claim 18 is similar to Claim 1 with more emphasis on the novelty of the platform certificate: confidentiality(encryption) is optional and therefore this step is decoupled from prevented modification and authentication (paragraphs [0032, 00100, 00104] and the MUX of Fig. 10). New dependent Claim 19 recites "the random key is directly used to encrypt the data"; support is found in fig. 10 (KEK) and paragraph [00100]. No new matter is introduced. In contrast to Applicants' invention, Ehrsam couples together modification prevention and authentication with encryption because Ehrsam does not have a switch to bypass one of the steps. Ehrsam also supports two levels of encryption (abstract host master key and file key, and claim 1, col 85, first and second master keys), whereby the random number is first encrypted by a so-called file key and then the electronic (e.g. data) file is encrypted by the encrypted random number. None of the elements of the new claims are taught by Pham. Therefore, Claims 18 and 19 should be allowable over the references.

New Claim 20 and 21 are directed towards the manufacture certificate which is not taught in the references. Support for Claim 20 is found in Table 1,

paragraphs [0032, 0040, 0055, 0056], figs. 2 and 4, and the corresponding text. No new matter is introduced.

Respectful request is made for reconsideration of the application, as amended, and for an issuance of a Notice of Allowance.

Respectfully submitted,

/Dolly Y. Wu/
Dolly Y. Wu
Reg. No. 59,192
Texas Instruments Incorporated
PO Box 655474, M/S 3999
Dallas, Texas 75265
972.917.4144